

The Digital Economy Bill: why National Pupil Data is the wrong model to copy

In theory: What the government says about its handling of personal confidential data, and why they do not accept a need for safeguards or oversight on the face of the Bill:

Lord Keen of Elie, Monday February 6, 2017 (Hansard)¹:

“We have to look at the provisions in this Bill in the context, first, of the Data Protection Act 1998, because the provisions of that Act apply in the context of this Bill. Therefore, as we look at the Bill, we must remember the protections that already exist in law with regard to data in this context. First, processing of personal data must always be fair and lawful. Secondly, data cannot be processed in a way that is incompatible with the purpose for which they were gathered. Thirdly, personal data must be,

“adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.

The personal data should be “accurate”, so a subject may be in a position to demand that they should be corrected.

Furthermore, on the point made by the noble Baroness, Lady Hamwee, personal data can be kept no longer than is necessary for a particular objective. Where, therefore, they have been employed for a particular objective—or a party has received them for a particular purpose—and a need to keep the data for that purpose can no longer be displayed, they cannot be retained.”

In practice: DfE policy and action do not respect today’s Data Protection Principles²

Schools, pupils and parents have no idea how their confidential records are used from the central database. It is processed for purposes parents and pupils do not expect, incompatible with the purpose they were collected. The public give personal information to schools with an expectation that it is used for the purposes of a child’s schooling and school administration, not that it is sent to a National Pupil Database (NPD) or that the Department for Education (DfE) gives away individual pupil-level, identifiable, confidential and sensitive data, collected in the termly school census.

The legal purposes “*for the purpose of promoting the education or well-being of children*” have been interpreted to mean giving out confidential, identifiable and sensitive data of individuals to third party users³ including data intermediaries and consultancies, a digital marketing agency, a private tutor pupil matching web service, and commercial companies creating web based products and services, like the Good Schools Guide which licenses some of its data for commercial re-use.

All of these are bulk data releases for millions of children’s identifiable confidential personal data, from the 20 million+ named records in the NPD, approved for release weekly by the DfE. From 1,364+ requests made between April 2012 and 2016, only 25 requests were rejected⁴.

Our children’s confidentiality is compromised. There is no consent process. There is no opt out.

There is no method to check data accuracy or get corrections, as the DfE refuses Subject Access Requests to enable parents or pupils to do so. The Department retains children’s personal data and school records forever without ability to have data removed after use ‘for a particular objective.’

If the Digital Economy bill permits similar wide data sharing of identifiable data without safeguards, it will create these same problems copied and pasted across all other datasets. There are valid reasons for using data in line with what the public trusts and expects, but without safeguards, this is misused.

¹ Hansard: <https://hansard.parliament.uk/lords/2017-02-06/debates/C19ED4AD-A46C-42F8-8162-D5B421F7CD8B/DigitalEconomyBill>

² <https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>

³ <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

⁴ source: written Parliamentary question 57722 <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-12-14/57722/>

Without safeguards on the face of the bill today's issues will be copied

1. Purposes “well-being” “promoting the education of children” “research” purposes:

The Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009 (Amended 2013) allows individual pupil information to be given to:

“persons who, for the purpose of promoting the education or well-being of children in England are

- (i) conducting research or analysis,*
- (ii) producing statistics, or*
- (iii) providing information, advice or guidance,*

and who require individual pupil information for that purpose.

For the purposes of these Regulations, ‘well-being’ has the meaning referred to in sections 332E and 507B of the Education Act 1996 in relation to those sections. Section 332E was inserted by section 1 of the Special Educational Needs (Information) Act [10]2008 (c.11) and section 507B was inserted by section 6(1) of the Education and Inspections Act [11]2006 (c.40).”

The public give their children's personal information to schools solely with the expectation that it is used for the purposes of their schooling and its administration, and perhaps national statistics.

Laws were changed in 2012-13 to allow individual level data to be released for broad purposes.⁵ The purposes which include ‘well-being’ and ‘research’ in the law that permits individual pupil data to be given out to third parties is open to interpretation of ‘prescribed persons’, similar in the DEBill.

These purposes “for the purpose of promoting the education or well-being of children” are now used to be able to give out confidential, identifiable and sensitive data of individuals to commercial third party users⁶ including data intermediaries and consultancies, a digital marketing agency, a private tutor pupil matching web service, and commercial companies, like the Good Schools Guide.

“Research” purposes has been interpreted to include the purposes of journalists from Fleet Street papers⁷ and television.⁸

2. Fair processing

Pupils and parent/guardians are not asked for consent and cannot refuse to have their data given away to third parties. There is no opt out of this data submission or its use.

This means that data are collected, retained forever, used without transparency and the public is unaware. In our 2014-15 research with over 500 schools and parents, under 2% knew and understood that their children's identifiable data is given away by the Department for Education for commercial use.

The total number of Unique Pupil Numbers (UPNs) in the NPD as at 28/12/2015 was 19,807,973. This covers pupil records of children in state education age 2-19, since 2000, and data since 1996.

The 12+ million people who have left school already, since Mr Gove changed the law to do so in 2012-13, have never been told that their data is being used for commercial purposes. The other 8 million, in school today, are supposedly informed via a privacy notice template⁹ posted on the DfE

⁵ <http://defenddigitalme.com/call-to-review-relevant-legislation/>

⁶ <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

⁷ <https://www.whatdotheyknow.com/request/293030/response/723407/attach/5/The%20Times.pdf>

⁸ <https://www.whatdotheyknow.com/request/293030/response/723407/attach/10/BBC%20Newsnight.pdf>

⁹ <https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notice>

webpage, but it doesn't effectively reach pupils and parents. The DfE make no mention of commercial use or use by journalists or that data are identifiable when released at pupil level.¹⁰

From age 2-19, since 2000, any state educated pupil's full school record in the NPD holds a lifetime record of named personal data, testing and tracking; attainment records, absence, opinions on reason for exclusions (alcohol, drugs, sex, theft, violence), indicators of armed forces or linked indicators of children in care. It is '*one of the richest education datasets in the world*' according to the National Pupil Database (NPD) User Guide. See [pages 19-22 of the User Guide](#).¹¹

From autumn 2016 more data were collected including country-of-birth and nationality from every child for the first time. This caused [controversy](#)¹² and led to a [#BoycottSchoolCensus campaign](#).¹³

3. Privacy and security

The Department for Education maintains that because the recipients sign user agreements that they will not onwardly share the data, and that they say they will meet certain security standards, that this means the data are secure and there is no breach of privacy.

This letter¹⁴ from The Telegraph offers "*cast iron assurances that no pupil will be identified from the use of the data.*" But the Telegraph [received](#) identifiable data, even if they do not publish it.

The Good Schools Guide (Lucas Publications) receives Tier 1 data (highly sensitive, identifiable individual level data). In their application they confirm they appreciate the risk of using the data:

"We will never share or publish individual-level data, and will ensure that the graphic representation of the data is executed in a way that no child or family will be identifiable. No exact postcode will be explicit, as we appreciate the sensitivity of being able to pin-point specific homes to schools and the protection [of] pupil identities will be paramount." [[Schools Guide, February 2014](#)]¹⁵

We view it is a breach of privacy at the point the DfE passes the data to the third parties outside the DfE and without consent, without informing the pupils and parents from whom the data comes. Parents and pupils expect that some data may be passed to the Department for Education. (DfE) The DfE privacy policy template offered to schools does not mention journalists, commercial use or data intermediary businesses. Even detailed privacy notices often omit onward sharing entirely.¹⁶

4. Retention

The Department once it receives pupils' data from the termly census keep the data forever, using the Data Protection Act 1998 exemption clause 33, because the Department considers this database a "research" database.

Third parties are sent millions of records including highly sensitive and individual-level pupil data. They keep it in their own locations. There is [no regular post-release oversight or audit process](#). When we enquired in July 2015, the Telegraph had not confirmed it had deleted personal data from the National Pupil Database that was over 18 months past its destruction date.

"Before July 2015, we did not have the data destruction notice in place and so do not currently hold this notice for the Daily Telegraph request in question. However, we received verbal confirmation that this data was deleted and are expecting the data destruction form to be returned to us shortly."

The Department has recently begun to audit, but how many of the 1000+ it will do is unknown.

¹⁰ <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data> DfE page accessed 07 Feb 2017 Data protection: how we share pupil and workforce data

¹¹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/472700/NPD_user_guide.pdf

¹² <http://defenddigitalme.com/press-coverage/>

¹³ <http://www.bbc.co.uk/news/education-38677439>

¹⁴ <https://www.whatdotheyknow.com/request/293030/response/738135/attach/2/Annex.pdf> The Telegraph compromise agreement to receive only sensitive, not 'highly' sensitive data

¹⁵ <https://www.whatdotheyknow.com/request/293030/response/723407/attach/11/School%20Guide%20UK.pdf>

¹⁶ <http://www.trinityfirstfrome.co.uk/perch/resources/policies/data-sharing-agreement-agreed-online-june-13-1.pdf>

Section 33 does not, however, give exemption to the remaining data protection principles which apply to personal data provided and/or used for research.

“Researchers wishing to use personal data should be aware that most of the data protection principles will still apply (notably the requirement to keep data secure) and, although the data subject’s consent to the processing is not always required, one of the other conditions relevant for the purposes of the fair and lawful processing of personal data will still be required where consent is absent. The First Data Protection Principle requiring personal data to be fairly and lawfully processed still needs to be adhered to, even if the ‘research exemption’ applies.” [ADRN, legal framework]¹⁷

5. Accuracy and right to have errors corrected

Parents are refused access to see their own children’s data, or to check whether it is accurate, or have it corrected if it is not. Subject Access Request rights are denied by the DfE on the basis of the exemption in the Data Protection Act 1998, Section 33, the same research based exemption. Accuracy matters because the database is used for direct interventions, incl. mail shots home¹⁸, or giving home address to the Removals Casework Team for Immigration Enforcement policy.¹⁹

6. Opinion: current laws, GDPR and children. Why s30 and Chapter 2 need change

If Clause 30 and Chapter 2 of the bill pass unchanged, the damage to public and professional trust in public data collection and use will be catastrophic, and risk harming public interest research.

These are sensitive data. Clause 30 (10)(a), refers to individuals’ “physical and mental health and emotional well-being” - that would cover school Special Needs records for example, an EHC (Education, Health and Care) plan when a formal SEN assessment has been made. These SEN indicators are given to journalists today. May these be shared with an even wider range of third parties without informing pupils or parents, in perpetuity, for reasons beyond direct care/school?

This kind of broad sharing and unlimited purposes fell down in the Supreme Court when it was challenged under **The judgment in the Named Persons case, “The Christian Institute and others (Appellants) v The Lord Advocate (Respondent) (Scotland)” in June 2016**. The Supreme Court judges said the law was “defective” for breaching article 8 of the European Convention on Human Rights (ECHR), which guarantees everyone’s “right to a private and family life”. They declared Holyrood had exceeded its powers by making a law which allowed public bodies to share sensitive private information about children and parents without consent.

The judges stated on the sharing of personal data, “*the operation of the information sharing provisions will result in interferences with the rights protected by article 8 of the ECHR*” (Para. 78). Because of the lack of safeguards “*the overriding of confidentiality is likely often to be disproportionate*” (Para. 100).

The Supreme court ruling for the Scottish Named Persons scheme reiterates DPA requirements: ‘For example, the second principle is that personal data must be “*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*”.’

The purposes of the school census collection, parents and pupils believe, are for their education. NOT to be handed out to commercial third parties, charities and press without their knowledge. We believe the national pupil data handling in England fails these similar tests today. Similarly therefore the Digital Economy Bill will fail these tests in future, and will be open to challenge.

This Bill s30 would permit data to be used just as pupil data has been since 2012: in bulk, for policy reasons, and in secret, without consent or informing the public from whom the data come.

¹⁷ ADRN legal framework, the S33 exemption and fair processing. Accessed 7 Feb 2017, <https://webcache.googleusercontent.com/search?q=cache:mafWUreURbAJ:https://adm.ac.uk/getting-data/resources/legal/dpa/+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b>

¹⁸ <http://content.digital.nhs.uk/article/3742/What-About-Youth-Study>

¹⁹ <https://arstechnica.co.uk/tech-policy/2016/12/uk-schoolkid-data-shared-create-hostility-against-illegal-migrants/>

National pupil data has been used monthly in secret for [immigration enforcement](#)²⁰ since July 2015, against lists of people, and without oversight or course of redress. What other policy reasons might the government give in future and use our data for in secret without telling us or Parliament?

The current **#BoycottSchoolCensus campaign**²¹ encouraging parents and pupils to refuse to participate in the nationality data collection, in schools, and the millions who opted out of care.data in health since 2014, demonstrate this risk is real, and risks further contamination through fear.

Sweeping data powers will no doubt be challenged in future, and the legality of the broad uses of pupil data need review²² not codifying through this bill. The use of pupil data for immigration enforcement, is likely contrary to **S.55 of the Borders, Citizenship and Immigration Act 2009**, that places a duty of regard for the children's welfare on the Home Secretary in these functions.

The Right to Education is protected by: Article 26 of **the Universal Declaration of Human Rights**, Articles 13 & 14 of **the International Covenant on Economic Social and Cultural Rights** and Articles 28,29 & 40 of **the UNCRC**. The Prime Minister planned policy to remove that in practice²³.

Everyone has the right to respect for his private and family life, his home and his correspondence, and the assessment of the "best interests of the child" is intrinsic to the proportionality assessment under the HRA Article 8.

Article 7 of the Charter of Fundamental Rights means everyone has the right to respect for his or her private and family life, home and communications, and Article 8 on the Protection of Personal Data means data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. And everyone has a right of access to data which has been collected, and right to have it rectified.

The Charter of Fundamental Rights Article 52 further requires that any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The upcoming **GDPR** (see p9) reiterates these fundamental freedoms and requires accountability and adequacy of data protection aligned with those Principles. The requirements for collection of children's data for processing by third parties and particularly with predictive scoring are not met in the school census collections. We have proposed a body of work to the DfE to get schools ready.

The GDPR requires consent documents to be laid out in simple terms. Silence or inactivity does not constitute consent; clear and affirmative consent to the processing of private data must be provided, it should not be open-ended or blanket consent to cover future processing.

Finally, Article 7(3) of the GDPR gives data subjects the right to withdraw consent at any time and *"it shall be as easy to withdraw consent as to give it."* That is currently not possible in the NPD for the few optional data, as most pupils are not offered consent, or do not know the database exists.

The Digital Economy Bill offers a chance to get this right. If it does not, then its failings on consent, fair processing, sweeping policy purposes for bulk data, Subject Access rights including correction and channels of redress, data minimisation and retention, will simply codify more policies and practice that need fixed to adequately respect children's data privacy rights before May 25, 2018.

²⁰ http://defenddigitalme.com/wp-content/uploads/2016/12/20161016_DfE-HO-MoU-redacted-copy.pdf

²¹ <http://schoolsweek.co.uk/human-rights-charity-warns-headteachers-over-pupil-nationality-data-collection/> Schools Week, Jan 15 2017

²² <http://defenddigitalme.com/call-to-review-relevant-legislation/>

²³ <http://www.bbc.co.uk/news/uk-politics-38165395>

7. Conclusion: Codifying today's problems makes the bill unfit for future

Lord Keen's remarks about the necessity of meeting today's principles: limitation of purposes, accuracy, right to correction and data minimisation, and respecting the rights of the individual being required under Data Protection Law such as to inform citizens and keep their data secure are true.

He spoke as if current government policy and practice already adheres to this, and claimed therefore we already have safeguards so the bill is fit for future. Neither position has basis in fact.

These protections for the citizen fail in today's government policy and practice by design, and will fail across further datasets, jeopardising further public trust, unless safeguards are put in place.

Government should not be seeking to create new laws to legitimise their current bad practices.

The risk is that the government policy will jeopardise or commoditise our children's confidentiality across every public administrative database by opening them up to broader purposes and future scope change at the whim of a Minister which won't require future scrutiny. HMRC data, DWP, Health, the Civil Registry of all birth, marriage and death registries and more. All our records could be about to be exposed to new uses without us ever being asked or told, in this new legislation.

There are plans to "join-the-dots" linking all children's data both direct care, and indirect secondary uses, across platforms from birth and the Early Years²⁴ to adulthood; in health, education, social services, HMRC, and DWP, driven by The Information Standards Board (ISB) at the DfE and BEIS, but yet again these ignore the views noted in its own report, "*young people's concerns about confidentiality and feeling in control of how, what, why, when and with whom information is being shared.*" (Gross, 2013b; Children and Young People's Health Outcomes Forum, 2015).^[p23/67] The HMRC database is soon to be used as the NCS marketing list to 15-17 year olds homes.²⁵

Without change the new legislation will continue to fail us tomorrow and be inadequate for GDPR. It is a missed opportunity that this bill does not address key requirements of GDPR for children: age verification and the age of consent²⁶, given that this topic is already part of the bill²⁷. Other countries already treat their children's data with greater respect of rights and human dignity.²⁸

The Digital Economy Bill and these policies create an unprecedented imbalance of State control and loss of citizens' privacy. It prioritises the economy, over our human rights, and autonomy.

Section 30 needs removed or to consider:

- a) duty to gain consent and enable a data subject to object and not have data shared on request
- b) a transparent register of all data access, users and purposes for every dataset
- c) complete and transparent register of all Back Office use (Home Office and Police)
- d) guaranteed Subject Access Request rights for any administrative data controller or processor
- e) duty to enable data correction of errors and make explicit channels of redress accessible
- f) duty to enable notification or audit after use, when a person's data is accessed or transferred (data usage reports could enable this, a mechanism to ensure trust in what is said will be done, is what is done with data) especially with regard to scope creep over time.

Chapter 2

The bulk sharing or bulk storage of birth, death, marriage, civil partnership documents must not be permitted - this enables a Stasi-like model of state control of citizens data at national level, and its data use must continue to have the most stringent of safeguards and required necessity of use, not opened up in general legislation for broad purposes at the policy whim of the Secretary of State.

²⁴ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/534744/Consistent_identifier_report_July_2016.pdf

²⁵ https://www.theyworkforyou.com/psc/2016-17/National_Citizen_Service_Bill/01-0_2017-01-24b.26.2#g26.4

²⁶ <http://blogs.lse.ac.uk/mediapolicyproject/2016/10/17/to-be-13-or-16-that-is-the-question-the-implications-for-uk-teenagers-of-the-european-general-data-protection-regulation/>

²⁷ <https://www.openrightsgroup.org/campaigns/digital-economy-bill-hub/age-verification/>

²⁸ <http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf> Protecting the Virtual Child, pp31-47, Dowty, T. and Korff, D.

8. Case studies: commercial access to pupil data since 2012²⁹

Innovative Consultancy: A digital marketing agency <https://www.weareinnovative.co.uk/>

Granted data on: 06/13/16 and can keep the data until: 30/04/2019

Level of individual pupil data granted: Tier 2 (pupil level, identifying and sensitive)

Download original request .pdf (188kB)³⁰

Requested purpose: To provide schools catchment area 'heat maps' for schools (Key Stage 2 – Key Stage 4, Key Stage 5). ICUK is looking to produce heat maps for pupil's admittance to any given school in the UK; this is to provide an additional public service to members of the public, showing general catchment area data, and to help parents gauge the likelihood of their child being granted admission to any given school based on their location. ICUK also aims to use Super Output Area and Distance to School measures data to provide a heat map/distance maps.

Tutor Hunt Ltd: Private personal tutors for private tuition <https://www.tutorhunt.com/>

"The *Tutor Hunt* network helps both tutors and students find each other."

Granted data on: 03/4/2015 and can keep the data until: 31/03/2017

Level of individual pupil data granted: Tier 1 (pupil level, identifying and highly sensitive)

Download original request .pdf (209kB)³¹

Requested purpose: Tutor Hunt was formed in 2005 and has slowly grown to be one of the largest tuition web sites within the United Kingdom with more than a quarter of a million registered users signed up. A large proportion of these registered users are parents. Tutor Hunt has created a schools guide, to help them review local schools (web page: <https://www.tutorhunt.com/schools/>). The schools pages give parents a comprehensive guide to local schools. One feature which Tutor Hunt are looking to add is to show a school's catchment area.

Good Schools Guide (Lucas Publications): <https://www.goodschoolsguide.co.uk/data>

Granted data on: 03/23/2016 and can keep the data until: 31/03/2019

Level of individual pupil data granted: Tier 1 (pupil level, identifying and highly sensitive)

Download original requests: **March 2016.pdf** (165kB)

Requested purpose: to analyse school performance, and to examine how well schools perform for different types of pupil and in different exam subjects, and to show where pupils come from and go to. The www.goodschoolsguide.co.uk website provides users with in-depth analysis of the data therefore all requested fields are needed in order to provide a sufficient level of information.

Concern: *The Good Schools Guide licenses some of its DfE supplied data for commercial use.*³² is this pupil level? The DfE does not charge commercial companies for access to pupil data (Written PQ 61684)³³. GSG charges for providing 'data and statistics'.³⁴

Schools Guide December 2014 (561kB) "The official school data provider to Mumsnet."³⁵

Granted data on: 16/12/2014

Other users include charities, journalists and academic public interest researchers. Case studies: http://defenddigitalme.com/wp-content/uploads/2016/04/DDM_shared_examples_April2016.pdf

²⁹ Sources: original FOI: https://www.whatdotheyknow.com/request/pupil_data_personal_data_release#outgoing-621858 forms sent by the DfE via private email to jen@defenddigitalme.com and as published in the DfE third party data recipients register <https://www.gov.uk/government/publications/national-pupil-database-requests-received> - Home Office and police use is omitted from this

³⁰ http://defenddigitalme.com/wp-content/uploads/2017/02/DR160222.02_Innovative-Consultancy.pdf

³¹ http://defenddigitalme.com/wp-content/uploads/2017/02/DR141203.01_TutorHunt.pdf

³² <https://www.goodschoolsguide.co.uk/data>

³³ <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-01-25/61684/>

³⁴ https://www.goodschoolsguide.co.uk/advice-service/school-data#tab_catchment

³⁵ Page 7 application form: <https://www.whatdotheyknow.com/request/293030/response/723407/attach/11/School%20Guide%20UK.pdf>

9. On School Census collection of nationality and country of birth data

Download our latest briefing including the Home Office DfE MOU on data sharing:
http://defenddigitalme.com/wp-content/uploads/2017/01/Briefing_DDM_11012017.pdf

Letters leaked to the BBC³⁶ reveal the purposes for which the expansion of the school census of country-of-birth and nationality and language detail are not simply what has been stated, but rather the collection was arranged as a compromise, and part of a package of measures at the request of the Home Office and Cabinet Office.

This policy decision was made at Immigration Taskforce discussions in July 2015: the “Department will gather pupil-level data on children’s country of birth, nationality and English proficiency through the school census from 2017.” The agreement was preceded by statements that the government was elected with a clear mandate, explicitly stated as “to bring down net migration”.

Since July 2015, over 2,462 requests³⁷ have been made by the Home Office of the NPD at the DfE, on a monthly basis, in which the Home Office presents lists of names to the DfE, which then returns school and home address data about individuals, their date of birth and gender.

The Memorandum of Understanding³⁸ first made public on December 15, 2016, and related information via FOI, revealed in Schools Week show the intent was to give pupil nationality data to the Home Office. This changed on Oct 7, 2016 (the day after the first collection of the new data) after campaign pressure from over 20 rights organisations and public scrutiny. Its purpose was in part to create a hostile environment [p14] and immigration enforcement. The previous agreement “did state that DfE would provide nationality information to the Home Office”, but that this was changed “following discussions” between the two departments.

It is important that parents are made fully aware of the purposes of these optional data, to ensure fair and legal collection by schools. A school’s statutory obligation to return data is met by returning the census data required fields containing valid data entries. Valid data entries include refused, not yet obtained, or unknown. The data themselves are optional.

Parents can choose not to provide the newly requested information in the 2016/17 school census: Country of Birth, Nationality, First Language

These data are optional, and not required: refused, not known and not yet obtained are valid returns for schools to use in these fields.³⁹ We believe most parents remain uninformed.

Since the purposes of the expanded census collection and the new use of school census data by the Home Office since 2015 have become clear after campaign pressure and press scrutiny, the National Union of Teachers has called for this use of pupil data to end, emphasising that “schools are not part of policing immigration”.⁴⁰

The national subject association for English as an Additional Language, NALDIC says, they “would like to urge the Department for Education to reconsider its position urgently” “...nationality should not be conflated with EAL proficiency. They are separate issues.”⁴¹

This divisive data policy decision was taken without public consultation or Parliamentary scrutiny.⁴²

³⁶ <http://www.bbc.co.uk/news/uk-politics-38165395>

³⁷ <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-10-13/48635/>

³⁸ http://defenddigitalme.com/wp-content/uploads/2016/12/20161016_DfE-HO-MoU-redacted-copy.pdf

³⁹ latest school census guidance from the Department for Education v1.5 published Jan 10, 2017

⁴⁰ <https://www.teachers.org.uk/news-events/press-releases-england/school-census-data>

⁴¹ <https://naldic.org.uk/assessment/eal-assessment-schools/school-census-returns/>

⁴² <http://defenddigitalme.com/wp-content/uploads/2016/09/Defenddigitalme-submission-SI2016-808.pdf>

10. GDPR recitals and articles relevant to children: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL⁴³

1. Article 6: lawfulness and legitimate interests and the interests of children
2. Article 7: right to withdraw consent at any time (for consent based data uses)
3. Article 8: parental consent
4. Article 12: transparent information provision
5. Article 17: right to erasure (commonly known as the Right to be Forgotten) and correction
6. Article 25: privacy by design
7. Article 35: data protection impact assessment
8. Article 40: codes of conduct
9. Article 57: DPAs awareness
10. Recital 38: specific protection
11. Recital 58: transparent information
12. Recital 65: right to erasure
13. Recital 71: profiling (relevant for Progress 8 school attainment forecasting)
14. Recital 75 : the risk to the rights and freedoms of natural /vulnerable persons

“The changes which are to be ushered in by the GDPR in 2018 are substantial and ambitious. At over 200 pages long the Regulation is one of the most wide ranging pieces of legislation passed by the EU in recent years, and concepts to be introduced such as the ‘right to be forgotten’, data portability, data breach notification and accountability.” Bird and Bird, January 2017 [[Guide to the GDPR, 2017](#)]⁴⁴

“The European Union has a historic opportunity to implement its new General Data Protection Regulation (GDPR) to ensure that there are meaningful controls for data gathered on youth. The largely unchecked role that data-driven digital marketing plays in the lives of adults is troubling enough. But we should all be concerned about its impact on young people.” Jeff Chester [[LSE Digital Parenting, January 2017](#)]

“it is urgent that the implementation of the General Data Protection Regulation that affects them is put high on the priority list of policymakers, children’s rights advocates, data protection authorities and industry.” Prof. Eva Lievens [[LSE Digital Parenting, 2016](#)]

See also Professor Sonia Livingstone’s extensive work on GDPR and children.⁴⁵

⁴³ http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

⁴⁴ <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>

⁴⁵ <http://blogs.lse.ac.uk/mediapolicyproject/tag/sonia-livingstone-2/>